Polityka ochrony danych osobowych (Polityka Bezpieczeństwa)

Polityka obowiązuje u: Beaty Siedlarz prowadzącej działalność nierejestrowaną.

Polityka obowiązuje od: 02.10.2024 rok

§ 1 Postanowienia ogólne

- Niniejsza Polityka ochrony danych osobowych (dalej: Polityka) stanowi ogólną regulację zasad i wymogów dotyczących ochrony danych osobowych (dalej: ochrona danych) obowiązujących u Administratora: Beaty Siedlarz ……, prowadzącej działalność nierejestrowaną pod adresem: Ptaszkowa 635, 33-333 Ptaszkowa
- Niniejsza Polityka, wraz z przywołanymi w niej dokumentami dotyczącymi ochrony danych, stanowi politykę ochrony danych w rozumieniu art. 24 ogólnego rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 roku r., w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.Urz.UE L119, s.1) (dalej: RODO).
- Polityka zawiera:
    - Opis zasad ochrony danych obowiązujących u Administratora: Beaty Siedlarz , prowadzącej działalność nierejestrowaną.
    - Odwołania do załączników uszczegóławiających (wzorcowe procedury lub instrukcje dotyczące poszczególnych obszarów z zakresu ochrony danych osobowych wymagających doprecyzowania w odrębnych dokumentach).

§ 2 Słowniczek pojęć

- **Dane osobowe**: pod tym pojęciem rozumie się, zgodnie z RODO, informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej (osobie której dane dotyczą); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora, takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.
- **Podmiot przetwarzający:** oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora.
- **Przetwarzanie danych osobowych:** oznacza, zgodnie z RODO, operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, takie jak: zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie,

adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie.

- **Polityka:** oznacza niniejszą Politykę ochrony danych osobowych.
- **RCPD:** oznacza Rejestr Czynności Przetwarzania Danych Osobowych.

§ 3 Podmioty odpowiedzialne

Osobą odpowiedzialną za wdrożenie i utrzymanie oraz nadzór i monitorowanie przestrzegania niniejszej Polityki oraz zasad ochrony danych osobowych jest Administrator: Beata Siedlarz prowadząca działalność nierejestrowaną.

§ 4 Zasady ochrony danych

- Zgodnie z przepisami RODO Administrator przetwarza dane osobowe na podstawie zasad określonych w art. 5 RODO.
- Administrator przetwarza dane osobowe z poszanowaniem następujących zasad:
    - W oparciu o podstawę prawną i zgodnie z prawem (legalizm)
    - Rzetelnie i uczciwie (rzetelność)
    - W sposób przejrzysty dla osoby, której dane dotyczą (transparentność)
    - W konkretnych celach (minimalizacja)
    - Nie więcej niż potrzeba (adekwatność)
    - Z dbałością o prawidłowość danych (prawidłowość)
    - Nie dłużej niż potrzeba (czasowość)
    - Zapewniając odpowiednie bezpieczeństwo danych (bezpieczeństwo)
- Wszelkie działania dotyczące ochrony danych osobowych winny mieć na względzie sformułowaną w RODO zasadę rozliczalności, nakazującą dokumentowanie przez administratora sposobu spełniania obowiązków tak, aby w każdej chwili móc wykazać zgodność z RODO.

§ 5 Upoważnienia do przetwarzania danych

- Wszystkie osoby dokonujące przetwarzania danych osobowych mogą działać jedynie na podstawie oraz w granicach polecenia i upoważnienia wydanego przez Administratora.
- Administrator prowadzi rejestr upoważnień.
- Podmioty zewnętrzne (dalej: Podmioty przetwarzające), a więc podmioty niedecydujące celach i sposobach przetwarzania danych, dokonują przetwarzania danych osobowych jedynie na podstawie oraz w granicach umowy powierzenia danych osobowych zawartych z Administratorem.
- Administrator prowadzi rejestr umów powierzenia.

§ 6 Rejestr czynności przetwarzania danych

- RCPD stanowi formę dokumentowania czynności przetwarzania danych, pełni rolę mapy przetwarzania danych i jest jednym z kluczowych elementów umożliwiających realizację fundamentalnej zasady, na której opiera się cały system ochrony danych osobowych, czyli zasady rozliczalności.
- Administrator prowadzi RCPD, w którym inwentaryzuje i monitoruje sposób, w jaki wykorzystuje dane osobowe.
- RCPD jest jednym z podstawowych narzędzi umożliwiających Administratorowi rozliczanie większości obowiązków ochrony danych.
- Administrator dokumentuje w RCPD podstawy prawne przetwarzania danych dla poszczególnych czynności przetwarzania.
- RCPD został stworzony w programie Excel z możliwością edytowania. RCPD jest dostępny **w załącznikach do niniejszej Polityki.**

§ 7 Obowiązki dotyczące praw osoby fizycznej

- Administrator dba o czytelność i styl przekazywanych informacji i komunikacji osobami, których dane przetwarza.
- Administrator ułatwia osobom korzystanie z ich praw poprzez różne działania, w tym: zamieszczanie na stronie internetowej Administratora informacji lub odwołań (linków) do informacji o prawach osób oraz sposobie skorzystania z nich.
- Administrator dba o dotrzymywanie prawnych terminów realizacji obowiązków względem osób.
- Administrator wprowadza adekwatne metody identyfikacji i uwierzytelniania osób dla potrzeb realizacji praw jednostki i obowiązków informacyjnych.
- W celu realizacji praw jednostki Administrator zapewnia procedury i mechanizmy pozwalające zidentyfikować dane konkretnych osób przetwarzane przez Administratora, zintegrować te dane, wprowadzać do nich zmiany i usuwać w sposób zintegrowany.
- Administrator dokumentuje obsługę obowiązków informacyjnych zawiadomień i żądań osób.
- Administrator spełnia względem osób, których dane przetwarza, obowiązek informacyjny – przekazuje wymagane prawem informacje przy zbieraniu danych (tzw. klauzule informacyjne).
- Osoba, której dane są przetwarzane, może w każdej chwili odwołać zgodę na przetwarzanie danych. Odwołanie zgody wywołuje wyłącznie skutki na przyszłość. W przypadku osób, które łączyła z Administratorem umowa, można przechowywać odpowiednio zabezpieczone dane w ilości niezbędnej do dochodzenia w przyszłości roszczeń z zawartej i realizowanej umowy, nie dłużej niż do czasu przedawnienia roszczeń lub odrębnych przepisów podatkowych.

- W razie zajścia przypadku naruszenia ochrony danych osobowych:
    - Naruszeniu bezpieczeństwa prowadzącym do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia albo zmodyfikowania danych osobowych;
    - Naruszeniu bezpieczeństwa prowadzącym do nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych obowiązuje ściśle określona w załącznikach do Polityki i zgodna z przepisami RODO procedura zgłaszania naruszenia danych oraz zawiadamiania osób, których dane dotyczą.
    - Administrator prowadzi rejestr naruszeń. Wzór tego rejestru jest dostępny w załączniku do niniejszej Polityki.
- Osobie, której dane dotyczą, przysługuje prawo do bycia zapomnianą. Prawo to polega na:
    - Możliwości żądania przez osobę, które dane dotyczą, usunięcia jej danych osobowych przez Administratora;
    - Możliwości żądania, aby Administrator poinformował innych Administratorów danych, którym udostępnił dane osobowe, że osoba, której dane dotyczą, żąda by administratorzy ci usunęli wszystkie łącza do tych danych lub ich kopie.
- Osobie, której dane dotyczą, przysługuje prawo do przenoszenia danych. Prawo to polega na możliwości żądania:
    - Otrzymania przez osobę, której dane dotyczą, w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynkowego, danych osobowych jej dotyczących, które dostarczyła Administratorowi;
    - Prawo żądania przez osoby, której dane dotyczą, przesłania danych osobowych jej dotyczących, które dostarczyła Administratorowi – innemu Administratorowi, bez przeszkód ze strony Administratora.
- Prawo do przenoszenia danych może być wykonane wyłącznie wtedy, gdy:
    - Przetwarzanie danych odbywa się na podstawie zgody lub w celu wykonania umowy oraz
    - Przetwarzanie danych odbywa się w sposób zautomatyzowany. Prawo do przenoszenia danych obejmuje tylko dane osobowe przetwarzane przy użyciu systemów informatycznych i nie obejmuje tradycyjnych, np. papierowych zbiorów danych.

§ 8 Okres przechowywania danych osobowych

- Jeżeli podstawą przetwarzania danych osobowych jest zgoda, dane osobowe mogą być przetwarzane tak długo, aż zgoda nie zostanie odwołana, chyba, że szczegółowe polityki stanowią inaczej.

- Jeżeli podstawą przetwarzania danych osobowych jest wykonanie umowy, dane osobowe mogą być przetwarzane tak długo, jak jest to niezbędne do wykonania umowy, a po tym czasie przez okres wynikający z obowiązku przechowywania danych księgowych i rachunkowych (na podstawie obowiązujących przepisów) lub przez okres niezbędny do dochodzenia lub przedawnienia roszczeń, jakie może ponosić Administrator lub jakie mogą być ponoszone w stosunku do Administratora.
- W pozostałych kwestiach okres przechowywania danych uregulowany jest osobnymi przepisami, które są respektowane przez Administratora.

§ 9 Bezpieczeństwo danych osobowych

- Należy mieć na uwadze, że przepisy RODO nie wskazują konkretnych środków zabezpieczenia danych osobowych.
- Administrator stosuje zasadę, że dobór środków bezpieczeństwa powinien być oparty na: stanie wiedzy technicznej, koszcie wdrażania, charakterze, zakresie, kontekście i celach przetwarzania, ryzyku naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia.
- Administrator, uwzględniając cel i kontekst przetwarzania danych osobowych, przeprowadził ocenę i analizę ryzyka, jakie wiąże się z ich przetwarzaniem; na tej podstawie zastosował odpowiednie środki techniczne i organizacyjne zabezpieczające dane (w tym w szczególności procedury i polityki, które są dostępne w formie załączników do niniejszej Polityki).
- Szacowanie oraz zarządzanie i analiza ryzyka odbywają się na podstawie ogólnego rozporządzenia o ochronie danych osobowych (RODO).
- Administrator wybiera takie metody szacowania ryzyka, które wpisują się w cały proces zarządzania działalnością nierejestrowaną i odpowiadają jej specyfice.
    - Administrator zapewnia odpowiedni stan wiedzy o bezpieczeństwie informacji, cyberprzestępstwie i ciągłości działania – wewnętrznie i ze wsparciem podmiotów wyspecjalizowanych.
    - Administrator kategoryzuje dane oraz czynności przetwarzania pod kątem ryzyka, które przedstawiają.
    - Administrator przeprowadza analizy ryzyka naruszenia praw lub wolności osób fizycznych dla czynności przetwarzania danych lub ich kategorii. Administrator analizuje możliwe sytuacje i scenariusze naruszenia ochrony danych osobowych, uwzględniając charakter, zakres, kontekst i cele przetwarzania, ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia.
- Administrator dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych tam, gdzie zgodnie z analizą ryzyka ryzyko naruszenia praw i wolności jest wysokie. Administrator stosuje metodykę oceny skutków przyjętą w swojej działalności nierejestrowanej.
- Administrator wdrożył też szereg procedur mających na celu realizację ciągłości działania.

.....

.....

Podpis Administratora

ZAŁĄCZNIKI:

- Wykaz technicznych i organizacyjnych środków bezpieczeństwa
- Procedura czystego biurka
- Procedura nadawania haseł
- Procedura postępowania w przypadku naruszenia ochrony danych osobowych
- Rejestr upoważnień
- Rejestr kategorii czynności przetwarzania
- Rejestr Czynności Przetwarzania Danych
- Rejestr naruszeń

Wykaz technicznych i organizacyjnych środków bezpieczeństwa

Zabezpieczenia techniczne stosowane w działalności nierejestrowanej prowadzonej przez: Beatę Siedlarz

- zbiór danych osobowych przechowywany jest w pomieszczeniu zabezpieczonym drzwiami zwykłymi (niewzmacnianymi, nie przeciwpożarowymi),
- pomieszczenia, w których przetwarzane są dane wyposażone są w system alarmowy przeciwwłamaniowy,
- dostęp do pomieszczeń objęty jest systemem kontroli dostępu,
- dostęp do pomieszczeń kontrolowany jest przez system monitoringu z zastosowaniem kamer przemysłowych,
- dane w formie papierowej przechowywane są w zamkniętej, niemetalowej szafie, kopie zapasowe/archiwalne danych osobowych przechowywane są w zamkniętej niemetalowej/metalowej szafie,
- pomieszczenia, w których przetwarzane są dane są zabezpieczone przed skutkami pożaru za pomocą systemu przeciwpożarowego i/lub wolnostojącej gaśnicy,
- dokumenty zawierające dane osobowe po ustaniu przydatności są niszczone w sposób mechaniczny za pomocą niszczarek dokumentów ręcznie nożyczkami poprzez pocięcie na bardzo małe części i wyrzucenie do kosza.
- dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła,
- dostęp do systemu operacyjnego komputera oraz telefonu, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem karty procesorowej oraz kodu PIN lub tokena
- zastosowano środki ochrony przed szkodliwym oprogramowaniem takim, jak np. robaki, wirusy, konie trojańskie, rootkity,
- użyto system Firewall do ochrony dostępu do sieci komputerowej,
- wykorzystano środki pozwalające na rejestrację zmian wykonywanych na poszczególnych elementach zbioru danych osobowych w systemie informatycznym,
- zastosowano środki umożliwiające określenie praw dostępu do wskazanego zakresu danych w ramach przetwarzanego w systemie informatycznym zbioru danych osobowych,
- dostęp do danych osobowych w systemie informatycznym wymaga uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła,
- zastosowano mechanizm wymuszający okresową zmianę haseł dostępu do systemu służącego do przetwarzania danych,
- zastosowano mechanizm automatycznej blokady dostępu do systemu informatycznego służącego do przetwarzania danych osobowych w przypadku dłuższej nieaktywności pracy użytkownika,

- szyfrowanie
- archiwizacja i tworzenie kopii zapasowych (backup) danych,
- wybór bezpiecznego hostingu , domeny i operatora płatności.

Zabezpieczenia organizacyjne stosowane w działalności nierejestrowanej prowadzonej przez: Beatę Siedlarz

- do przetwarzania danych zostały dopuszczone wyłącznie osoby posiadające upoważnienie,
- prowadzona jest ewidencja osób upoważnionych do przetwarzania danych,
- została opracowana i wdrożona polityka bezpieczeństwa,
- została opracowana i wdrożona instrukcja zarządzania systemem informatycznym,
- kopie zapasowe zbioru danych osobowych przechowywane są w innym pomieszczeniu niż to, w którym znajduje się serwer, na którym dane osobowe przetwarzane są na bieżąco,
- polityka czystego biurka,
- polityka czystego ekranu,
- procedura nadawania haseł,
- procedura szacowania ryzyka,
- procedura archiwizacji oraz usuwania dokumentów zawierających dane osobowe,
- procedura logowania do systemów IT oraz korzystania ze służbowej poczty elektronicznej,
- procedura konserwacji i serwisowania urządzeń,
- procedura postępowania w przypadku naruszenia bezpieczeństwa danych osobowych.

Polityka czystego biurka

1. Polityka czystego biurka obowiązuje wszystkich mających dostęp do danych osobowych przetwarzanych w działalności nierejestrowanej prowadzonej przez: Beatę Siedlarz i jest częścią Polityki Ochrony Danych obowiązującej od 02.10.2024..

2. Za pracowników uważa się każdą osobę zatrudnioną na podstawie stosunku pracy, a także zleceniobiorców, stażystów, praktykantów, osoby współpracujące oraz samozatrudnione na rzecz administratora danych, tj. Beata Siedlarz.

3. Każda osoba mająca dostęp do danych osobowych przetwarzanych w ramach działalności nierejestrowanej, prowadzonej przez: Beatę Siedlarz jest zobowiązana jest do przechowywania na biurku tylko tych dokumentów, które są mu niezbędne do pracy w danym momencie. Należy unikać przechowywania dokumentów niepotrzebnych do bieżących zadań.

4. Po zakończeniu pracy z dokumentami zawierającymi dane osobowe należy odłożyć je do szuflady.

5. Dokumenty niepotrzebne w dalszej pracy i niepodlegające archiwizacji należy niszczyć zgodnie z zaleceniami „Procedury niszczenia dokumentów” np. w niszczarce.

6. Ekrany monitorów komputerów powinny być ustawione tak by uniemożliwiały widok osobom postronnym.

7. Na biurku nie powinny znajdować się napoje w pojemnikach grożących rozlaniem.

8. Po zakończeniu pracy na biurku powinny pozostać tylko komputer, telefon i przybory biurowe.

9. Niniejsza Polityka obowiązuje od dnia 02.10.2024.

Procedura nadawania haseł

Celem procedury jest zapewnienie, że do systemów informatycznych przetwarzających dane osobowe mają dostęp jedynie osoby do tego upoważnione.

1. Pierwsze (pierwotne) hasło użytkownika nadawane jest przez administratora i przekazywane mu w poufny sposób.

2. Standard hasła: do każdego programu/systemu – hasło co najmniej 8 znaków (duże, małe litery, cyfry i znaki specjalne) / do poczty służbowej: hasło 12 znaków (duże, małe litery, cyfry i znaki specjalne). Zmiana hasła jest wymuszana przez system . Użytkownicy są zobowiązani do samodzielnej zmiany hasła jeśli system tego nie wymaga.

3. Administrator nie ma dostępu do haseł użytkowników za wyjątkiem haseł do stacji roboczych.

4. Hasła do stacji roboczych winny być zgodne z polityką haseł i przekazane do działu informatyki w celu zabezpieczenia w razie potrzeby dostępu do stacji roboczych.

5. W sytuacji zapomnienia przez użytkownika swojego hasła, administrator przywraca hasło do ustawień początkowych i przekazuje go użytkownikowi celem niezwłocznej późniejszej zmiany.

6. Zastosowano mechanizm blokady dostępu po 5 próbach nieudanego logowania się.

7. Hasła administracyjne zdeponowane są w bezpiecznym miejscu.

8. W przypadku utraty uprawnień przez osobę administrującą systemem należy niezwłocznie zmienić hasła, do których miała dostęp.

Procedura postępowania w przypadku wystąpienia zdarzenia mogącego powodować zagrożenie dla bezpieczeństwa danych osobowych.

- Procedura obowiązuje w działalności nierejestrowanej prowadzonej przez: Beatę Siedlarz, będącą Administratorem.
- Procedura obowiązuje od: 02.10.2024.

§ 1 Informacje wstępne

1. Zgodnie z przyjętą w dniu 02.10.2024, Polityką ochrony danych osobowych w Administratora: Beatę Siedlarz, prowadzącego działalność nierejestrowaną, prowadzony jest Rejestr zdarzeń (incydentów i naruszeń) bezpieczeństwa danych osobowych i obowiązuje od dnia:02.10.2024.
2. Celem niniejszej procedury jest zapewnienie, że zdarzenia (incydenty i naruszenia) związane z bezpieczeństwem informacji oraz słabość systemów informatycznych są zgłaszane w sposób umożliwiający szybkie podjęcie działań korygujących, by chronić prawa i wolności osób, których dane są przetwarzane.
3. Za prowadzenie i aktualizowanie rejestru odpowiada Administrator.

§ 2 Przedmiot i zakres procedury

1. Incydent bezpieczeństwa do zdarzenie lub seria zdarzeń, które bezpośrednio zagrażają bezpieczeństwu informacji, w szczególności takim aspektom jak zachowanie poufności, integralności i dostępności danych.
2. Za naruszenie zasad ochrony danych osobowych uważa się w szczególności:

    - nieupoważniony dostęp, modyfikację, kopiowanie lub zniszczenie/usunięcie danych osobowych, zarówno w systemie informatycznym, jak i na nośnikach papierowych i elektronicznych,
    - udostępnianie danych osobowych nieuprawnionym podmiotom lub osobom,
    - nieautoryzowany dostęp do danych przez połączenie sieciowe,
    - dostęp do pomieszczeń, w których przetwarza się dane osobowe dla osób nieuprawnionych
    - niedopełnienie obowiązku ochrony danych osobowych przez umożliwienie dostępu do danych (np. pozostawienie kopii danych, niezablokowanie dostępu do systemu, brak nadzoru nad serwisantami i innymi osobami nieuprawnionymi przebywającymi w pomieszczeniach gdzie przetwarza się dane osobowe,
    - wykrycie niezabezpieczonego kanału dystrybucji danych osobowych,
    - nielegalne bądź nieświadome ujawnienie danych osobowych,
    - pozyskiwanie danych osobowych z nielegalnych źródeł,
    - przetwarzanie danych osobowych niezgodne z uprawnionym celem i zakresem,

- stwierdzenie obecności wirusów komputerowych lub innych programów godzących w integralność systemu informatycznego,
- ujawnienie indywidualnych haseł dostępu do systemu,
- przesyłanie danych osobowych przez Internet bez zabezpieczenia,
- przesyłanie dokumentów papierowych i nośników elektronicznych z danymi bez zabezpieczenia,
- wykonanie nieuprawnionych kopii danych osobowych,
- naruszenie bezpieczeństwa kopii danych osobowych,
- kradzież nośników zawierających dane osobowe lub oprogramowanie,
- kradzież sprzętu służącego do przetwarzania danych osobowych,
- utratę danych osobowych w systemie informatycznym, na kopiach bezpieczeństwa i na innych nośnikach,
- brak aktualnych kopii bezpieczeństwa danych osobowych lub brak odpowiednich nośników do sporządzania kopii,
- niewłaściwe niszczenie nośników z danymi osobowymi pozwalające na ich odczyt,
- naruszenie zasad ochrony fizycznej pomieszczeń, w których przetwarza się dane osobowe,
- inne sytuacje wskazujące lub potwierdzające naruszenie bezpieczeństwa danych osobowych.

3. Incydenty naruszenia można sklasyfikować jako: incydenty losowe zewnętrzne, incydenty losowe wewnętrzne, incydenty umyślne.

§ 3 Opis postępowania

1. W przypadku stwierdzenia naruszenia bezpieczeństwa danych należy zaniechać wszelkich działań mogących utrudnić analizę wystąpienia naruszenia i dokumentowanie zdarzenia.
2. W celu przeprowadzenia analizy zdarzenia Administrator podejmuje następujące działania:
    - Zapoznaje się z zaistniałą sytuacją – ustala oznaki naruszenia bezpieczeństwa, identyfikuje rodzaj incydentu, identyfikuje i zabezpiecza dowody.
    - Wybiera sposób dalszego postępowania, uwzględniając zagrożenie prawidłowości funkcjonowania działalności nierejestrowanej.
    - Może zażądać dokładnej relacji z zaistniałego naruszenia bezpieczeństwa danych osobowych od każdej osoby, która może posiadać informacje w związku z zaistniałym naruszeniem.
    - W przypadku uznania danego zdarzenia za incydent bezpieczeństwa informacji dokonuje oceny istotności incydentu.
    - Administrator ocenia poziom istotności incydentu dla prowadzonej działalności nierejestrowanej, kierując się następującymi kryteriami:
        - Wpływ incydentu na ciągłość działania działalności nierejestrowanej i realizacji zadań przedsiębiorcy.

- Krytyczność systemów dotkniętych skutkami incydentu bezpieczeństwa.
- Wrażliwość informacji, których poufność, integralność czy dostępność naruszono.
- Rozległość wpływu incydentu na działanie systemów.
- Rozmiar powstałych szkód.
- Koszt usunięcia i naprawy skutków incydentu bezpieczeństwa.
- Szacowanego czasu przywrócenia ciągłości działania dotkniętego incydentem bezpieczeństwa systemu.
- Zasoby wymagane do przywrócenia ciągłości działania systemu.

3. Administrator nawiązuje kontakt ze specjalistami spoza prowadzonej działalności nierejestrowanej (jeśli zachodzi taka potrzeba).
4. Administrator wprowadza działania naprawcze zmierzające do zniwelowania szkód wyrządzonych przez incydent, wyciąga wnioski z każdego incydentu i określa, jeśli to możliwe, działania korygujące i zapobiegawcze w celu uniknięcia ponownego wystąpienia incydentu (w tym także ustosunkowuje się do kwestii ewentualnego odtworzenia danych z zabezpieczeń oraz terminu wznowienia przetwarzania danych osobowych).
5. Administrator prowadzi rejestr naruszeń bezpieczeństwa danych osobowych:
    - Rejestr jest prowadzony w formie elektronicznej i papierowej.
    - Do rejestru naruszeń wpisywane są wszystkie incydenty i naruszenia związane z ochroną danych osobowych.
    - Rejestr jest prowadzony na podstawie obowiązku wynikającego z ert.33 ust.5 RODO.
6. Administrator w razie stwierdzenia, że dany incydent bezpieczeństwa powoduje wysokie ryzyko naruszenia praw lub wolności osób, których dane są przetwarzane, zawiadamia organ nadzorczy, tj. Prezesa Urzędu Ochrony Danych Osobowych do 72 h o tym naruszeniu.
7. Zawiadomienie PUODO o naruszeniu zawiera:
    - Charakter naruszenia, w tym w miarę możliwości należy wskazać kategorię i przybliżoną liczbę osób, których dane dotyczą,
    - Dane Administratora,
    - Konsekwencje naruszenia
    - Środki podjęte w celu zaradzenia naruszeniu ochrony danych.